

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



21

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :	A1	(11) International Publication Number: WO 00/20950
G06F 1/00		(43) International Publication Date: 13 April 2000 (13.04.00)

(21) International Application Number: PCT/US99/23474

(22) International Filing Date: 7 October 1999 (07.10.99)

(30) Priority Data:
09/167,888 7 October 1998 (07.10.98) US

(71) Applicant: GLASSBROOK, INC. [US/US]; Suite 107, 179 Great Road, Acton, MA 01720 (US).

(72) Inventors: KAWELL, Leonard, M., Jr.; Concord, MA (US). DIAZ, Thomas, R.; Lexington, MA (US). HEINEN, Mary, Ellen; Concord, MA (US). HEINEN, Rodger, J., Jr.; Islesboro, ME (US).

(74) Agents: REYES, Jason, A. et al.; Hale and Dorr LLP, 60 State Street, Boston, MA 02109 (US).

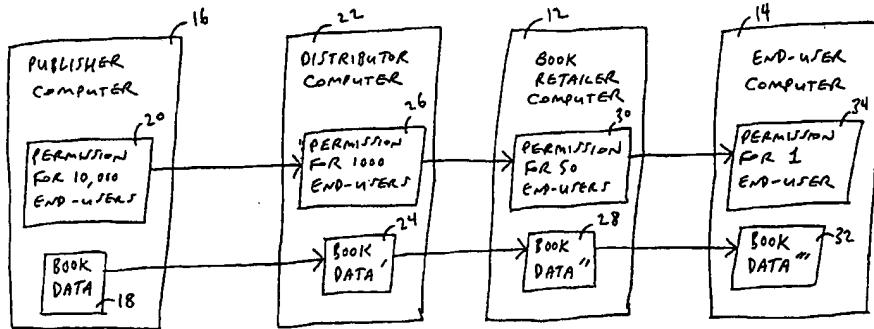
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: DISTRIBUTING ACCESS TO A DATA ITEM



(57) Abstract

A method is provided for use in distributing access to a data item. The method includes allowing multiple transfers between computers of a single instance of permission to gain access to the data item, the transfers occurring across data connections and including a first transfer between a first computer and a second computer and a subsequent transfer between the second computer and a third computer, wherein at any one time only one computer retains the instance of permission and is able to use the instance of permission to gain access to the data item.

DESI AVAILABILITY COPY

BEST AVAILABLE COPY

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

1

DISTRIBUTING ACCESS TO A DATA ITEM

Background of the Invention

A computer data item such as a file that contains the text of a book or

5 an arrangement of data that represents an audio or video rendering or recording may be copied and distributed via removable media such as a floppy diskette or a CD-ROM or over a computer network such as the Internet. In some cases, a data item is intended to be copied and distributed freely, with

10 little or no control over access to the data item. In other cases, control over access is attempted by physical means, such as by exercising some control over the number of pieces of removable media that are produced, or by copy protection methods that impede the ability of a computer to produce a copy of

15 the data item.

As shown in Fig. 1, in existing electronic book distribution systems, a data item that represents the contents of a book ("book data") is copied (e.g.,

20 across a network connection) from a central source to book reading devices (i.e., book viewing devices) in a hub-and-spoke arrangement.

Summary of the Invention

In general, in one aspect, the invention features a method for use in

25 distributing access to a data item. The method includes allowing multiple transfers between computers of a single instance of permission to gain access to the data item, the transfers occurring across data connections and including a first transfer between a first computer and a second computer and a

30 subsequent transfer between the second computer and a third computer, wherein at any one time only one computer retains the instance of permission and is able to use the instance of permission to gain access to the data item.

Implementations of this or another aspect of the invention may include one or more of the following features. The method may include using an encryption key to impede unauthorized access to the data item. At least one of the transfers of permission may include the transfer of a first encryption key, and the method may include using a second encryption key to encrypt the first encryption key prior to transfer. The first encryption key may include a secret key and the second encryption key may include one of the keys in a public/private key set. The method may include using highly secure circuitry to help ensure that at any one time only one of the computers retains and is able to use the instance. The highly secure circuitry may include a smartcard computer or a de-encryptor. The method may include storing an encryption key in the highly secure circuitry, and may include using the encryption key only within the highly secure circuitry. The method may include determining whether a computer is authorized to receive the instance of permission to gain access to the data item, or, according to an expiration time, rendering at least one of transfers temporary. The method may include, in the temporary transfer, transmitting a copy of an encryption key from a sender computer to a recipient computer, and, at the expiration time, erasing the copy of the encryption key from the recipient computer. The method may include, in one of the transfers, transmitting a copy of an encryption key from a sender computer to a recipient computer, and erasing the copy of the encryption key from the sender computer. The method may include associating at least one of the transfers with a transfer of funds, or distinguishing between different instances of permission to gain access to the data item. At least one of the computers may include a Web server computer or a book viewing device. The

book viewing device may include a viewing screen and data communications circuitry.

In general, in another aspect, the invention features a method including:

5 in accordance with access distribution parameters that are specific to a data item and that were established by a first computer, transferring, across a data connection from a second computer to a third computer and independently of the first computer, permission to gain access to the data item.

10 In general, in another aspect, the invention features a method including: impeding a change to the number of computers that are allowed to gain access to a data item, independently of data connection transfers between computers of permission to gain access to the data item.

15 In general, in another aspect, the invention features a method for use in distributing access to a data item. The method includes providing a first computer with permission to gain access to the data item; providing the permission by data connection to a second computer substantially simultaneously with removing the permission from the first computer; and providing the permission by data connection to a third computer substantially simultaneously with removing the permission from the second computer.

20 In general, in another aspect, the invention features a method including: rendering accountably fungible an instance of permission data that allows a computer to gain access to book data.

25 In general, in another aspect, the invention features a method for use in distributing access to a book data item. The method includes associating highly secure circuitry with a device that is able to send and receive access data that is necessary to gain access to the book data item, the highly secure

30 In general, in another aspect, the invention features a method for use in distributing access to a book data item. The method includes associating highly secure circuitry with a device that is able to send and receive access data that is necessary to gain access to the book data item, the highly secure

circuitry including a computer processor and a program memory and being able to substantially prevent an unauthorized transfer of the access data from the device.

5 In general, in another aspect, the invention features a method for use in distributing access to a book data item. The method includes: at a publisher computer, storing publisher permission data that allows a number A of end-user computers to gain access to the book data item; based on the publisher permission data, providing a distributor computer with distributor permission data that allows a number B of end-user computers to gain access to the book data item; changing the publisher permission data so that the publisher permission data allows only a number A-B of end-user computers to gain 10 access to the book data item; based on the distributor permission data, providing a retailer computer with retailer permission data that allows a number C of end-user computers to gain access to the book data item; changing the distribution permission data so that the distributor permission data allows only a number B-C of end-user computers to gain access to the book data item; based on the retailer permission data, providing an end-user computer with end-user permission data that allows 1 end-user computer to 15 gain access to the book data item; and changing the retailer permission data so that the retailer permission data allows only a number C-1 of end-user computers to gain access to the book data item.

20

25

30 Among the advantages of the invention are one or more of the following. Access to a data item (i.e., permission to use the data item) can be controlled without excessively burdening users (e.g., consumers) of the data item or excessively hindering the scalability of distribution by traditional data

copying techniques. In at least some cases, acquiring the data item under authorization can be made easier than acquiring a corresponding physical rendering (e.g., a paper book or a music compact disc), and nearly instant gratification can be achieved for the end-user. Access to the data item can be made fungible and therefore valuable. The distribution of works (e.g., books, audio recordings, pictures) can be limited in number without conventional reliance on physical manufacturing, which limiting can help maintain the value of the works. An accounting can be made of the number of end-users that have access to a data item. An entity can lend a data item to an end-user much as a library lends a book. A data item can be transferred across a data connection but can made fully usable regardless of whether the data connection is available at the time of use. Full or nearly full advantage may be taken of the Internet and the World-Wide Web in the distribution of access to a data item.

Other features and advantages will become apparent from the following description, including the drawings, and from the claims.

Brief Description of the Drawings

Fig. 1 is a block diagram of a prior art book data distribution system in which book reading devices receive book data directly from a central source.

Fig. 2 is a block diagram of a book data distribution system in which book data is passed from a publisher computer to distributor computers to retailer computers to end-user computers.

Fig. 3 is a block diagram of transfers of permission among publisher, distributor, retailer, and end-user computers.

Fig. 4 is a block diagram of transfers of permission data among user computers.

Fig. 5 is a flow diagram of a usage permission transfer procedure.

5 Fig. 6 is a block diagram of a smartcard computer.

Fig. 7 is a block diagram of groups and private keys.

Figs. 8-11 are block diagrams of data flows in a usage permission transfer procedure.

10 Figs. 12-14 are flow diagrams of a usage permission transfer procedure.

Fig. 15 is an illustration of a book viewing device.

Detailed Description

15 Fig. 2 illustrates a controlled data distribution system 10 in which a data item such as data including the text of a book ("book data") is distributed from a sender computer (e.g., retailer computer 12) to a recipient computer (e.g., end-user computer 14) in accordance with distribution control parameters determined at least in part by an originating computer (e.g., publisher computer 16), regardless of whether the originating computer is available at the time of the distribution from the sender computer to the recipient computer. Thus, distribution is not only convenient but also private, because in at least some cases the only computers that ever have any information about a particular instance of distribution are the sender computer and the recipient computer.

25 30 Fig. 3 shows a general example in which an original copy 18 of a book data item is held at the publisher computer which has permission data 20 to allow up to 10,000 end-user computers (e.g., book reader computers) to have

access to the book data item. In such a case, the publisher computer provides a distributor computer 22 with a copy 24 of the book data item and permission data 26 to allow access by 1,000 end-user computers, which leaves the 5 publisher computer with permission data to allow access by 9,000 end-user computers. Further, in turn, the distributor computer provides the retailer computer with a copy 28 of the book data item and permission data 30 to allow access by 50 end-user computers, and the retailer computer provides 10 end-user computer 14 with a copy 32 of the book data item and permission data 34 to allow access. Thus, the publisher, distributor, retailer, and end-user computers form a distribution network in which permission is distributed from the publisher computer to end-user computers much as printed books are 15 distributed from a print publisher to consumers in a printed book distribution system: permitted access may be regarded as a fixed resource such that the maximum number of end-user computers that are allowed to gain access to the 20 book data item is not affected by distribution.

As shown in Fig. 4, controlled distribution as described above need not take place in a hierarchy (e.g., from publisher computer down to end-user computers), and may occur between any two computers that execute according 25 to a usage permission transfer procedure 36 illustrated in Fig. 5 (a more detailed example is described below in connection with Figs. 8-14). At the sender computer (e.g., User A's computer 38), it is determined whether the recipient computer (e.g., User B's computer 40) has been certified by an 30 organization that certifies devices intended to make use of data items, and is therefore authorized to be granted access to the data item (e.g., item 42) (step 1010). The purpose of the organization is to help ensure that only devices that

conform to rules of the organization are allowed to gain access to data items associated with the organization. For example, the organization may not certify a device that lacks a highly secure clock or a highly secure program 5 memory, or that has not been demonstrated to use encryption tools reliably.

If the recipient computer has been certified, the sender computer transmits permission data (e.g., usage permission data B based on usage permission data A) in a highly secure way to the recipient computer (step 10 1020). If a copy of the data item is stored at the sender computer, a copy of the data item (e.g., data item 44) may be transmitted in a highly secure way from the sender computer to the recipient computer (step 1030). The recipient computer gains access to the data item in accordance with the permission data 15 (step 1040).

It is important that formulation and transmission of the permission data be accomplished in a highly secure way, because control over distribution 20 depends on such formulation and transmission being performed only under authorized conditions. While it may be impossible to completely block unauthorized actions by determined actors with significant resources (e.g., professional pirates), high security can be effective to help to discourage others 25 (e.g., student hackers), and to help to make clear that the distribution is intended to be controlled and is not intended to add the data item to the public domain.

To help ensure high security, each of the sender computers and recipient 30 computers may rely on encryption devices known as secret keys and public/private key sets, and may include a highly secure mechanism, which may handle one or more of the keys or key sets, or encrypted or unencrypted

data, or both. A secret key (also known as a symmetric key) is a string of data (e.g., 40 bits) that may be used to encrypt other data in a way that allows the other data to be de-encrypted using the same secret key. A public/private key set includes two strings of data (e.g., 1024 bits each) that cannot be derived from each other and that are matched such that other data that has been encrypted by using either one of the two strings can be de-encrypted only by using the other of the two strings. Typically, one of the two strings ("public key") is not kept confidential and the other of the two strings ("private key") is kept highly confidential. See Public Key Cryptography Standards, RSA Laboratories, Security Dynamics, Inc., Nov. 1993, and RSA Public Key Crypto System, RSA Data Security Division, Security Dynamics, Inc., 1982.

A conventional general-purpose computer can be used to generate the secret key and the public/private key set, which can be stored in conventional computer files, as can data that has been or is intended to be encrypted by using one or more of the keys. In at least some cases, security is enhanced if the highly secure mechanism handles the keys and includes a smartcard computer 46 (Fig. 6) (e.g., a Gemplus GemXpresso), which is physically sealed to impede unauthorized access to internal components, and has connection circuitry 48 that provides the only authorized means for exchanging data with circuitry outside the smartcard computer. The smartcard computer also has a program memory 50, a data memory 52, and a processor 54 that communicates with the connection circuitry and executes according to software stored in the program memory to implement a public/private key encryptor 56, a public/private key de-encryptor 58, a secret key encryptor 60, and a secret key de-encryptor 62. A permission data bank 64, a public key 66, a private key 68,

and a digital signature 70 are stored in the data memory (e.g., when the smartcard computer is manufactured). The digital signature (also referred to as the encrypted digest) is the result produced by generating a digest version 5 of the public key (e.g., by applying a hash function to the public key) and then using a group private key (Fig. 7) to encrypt the digest version.

Each smartcard computer's public/private key set is different (i.e., unique), but the group private key is the same for every smartcard computer 10 in a group. In a specific embodiment, the smartcard computer also stores an identification of the entity with which the smartcard computer is associated, if the entity is a publisher, distributor, or retailer, and stores an anonymous serial number instead if the entity is an end-user (e.g., a consumer), to help 15 protect the privacy of the end-user. In alternative versions of the specific embodiment, the digital signature is supplemented or replaced by a digital certificate, which is the result created by using the group private key to 20 encrypt the identification.

The smartcard computer may be able to execute software programs formatted according to a programming language known as Java.

In a specific embodiment, only the publisher computer is provided with 25 a secret key encryptor (e.g., because the other computers are not originators of encrypted data items) and only the end-user computer is provided with the secret key de-encryptor (e.g., because the other computers do not display or otherwise make significant use of the data items).

30 Figs. 8-14 illustrate a detailed example 72 of the usage permission transfer procedure. A secret key 74 (e.g., a randomly-generated 40-bit number) is used to encrypt book data 76 to produce secret key encrypted book data 78

(step 2010), which is stored at a sender computer (step 2020). (In a specific embodiment, the secret key is also appended to the secret key encrypted book data.)

5 The encrypted digest and the recipient computer's unique public key are transmitted from the recipient computer to the sender computer (steps 2050, 2060). At the sender computer, a group public key 84 is used to de-encrypt the encrypted digest to produce a de-encryption result 86 (step 2070), and a digest 10 result 88 is produced from the recipient's unique public key (step 2080). At the sender computer, the digest result is compared to the de-encryption result to determine whether the recipient computer has been certified as described above and is therefore authorized to receive book data (step 2090), and if it is 15 determined that the recipient computer has not been certified, the recipient computer's requests for book data are refused (step 2100).

20 As shown in Fig. 10, a request for book data 90 and the recipient computer's unique public key are transmitted from the recipient computer to the sender computer (steps 2110, 2120). (In a specific embodiment, the request is associated at the recipient computer with a unique request serial number and with a request expiration time such as 60 seconds so that the request is 25 cancelled at the request expiration time if a response is not received from the sender computer in time, and any response from the sender computer to the request is associated with the same unique request serial number so that the response can be matched to the request at the recipient computer.) At the 30 sender computer, secret key encrypted book data and a secret key and voucher corresponding to the request are selected (step 2130), and the recipient's unique public key is used to produce a public key encrypted secret key and voucher

94 (step 2140), which is transmitted along with the secret key encrypted book data to the recipient computer from the sender computer (steps 2150, 2160).

At the recipient computer (Fig. 11), the recipient's unique private key is
5 used to produce a secret key and voucher 98 (step 2180), and the secret key is used to produce unencrypted book data 100 from the secret key encrypted book data (step 2190).

At this point, the unencrypted book data may be displayed or otherwise
10 used at the recipient computer.

In at least some cases, it may be advantageous if the unencrypted book data is in a format (e.g., a version of an Adobe format known as Portable Document Format or "PDF") that allows the data to be displayed in a specified
15 way (e.g., by Adobe display software) but renders printing the data or reformatting the data difficult or impossible. See Portable Document Format Reference Manual, Version 1.2, November 1996, Adobe Systems, Inc. Thus, the
20 originator of the unencrypted book data (e.g., a publisher) can have a high degree of confidence that the integrity of the book data will survive distribution and that the book data will be displayed in accordance with the originator's intent (e.g., in the intended fonts and type sizes and with intended
25 line and page breaks).

The usage permission transfer procedure may be applied when permission to use a data item is lent (e.g., by a library), leased, given (e.g., as a birthday present), or sold (e.g., by a book retailer). If the permission is lent or
30 leased, the procedure also specifies that the secret key is associated with matching expiration times 102S and 102R (e.g., each corresponding to a two-week period) at the sender and recipient computers, respectively, so that the

secret key cannot be used (and therefore the data item cannot be used) at the sender computer until expiration time 102S is reached, and can be used at the recipient computer only until expiration time 102R is reached. In this way, the 5 permission is effectively returned to the sender computer from the recipient computer when the expiration time is reached. If the sender computer or the recipient computer has permission data for multiple end-user computers for the same data item (e.g., in the case of a library that is able to lend to multiple 10 end-user computers), matching serial numbers 104S and 104R are retained in each lend or lease transaction so that different instances of permission may be distinguished from each other. The voucher specifies the expiration times and 15 the serial numbers, and also specifies a quantity 106 if the recipient computer is to be provided with permission data to allow more than one end-user computer to gain access to the data item (e.g., where a publisher computer provides a distributor computer with permission data with respect to 50 end- 20 user computers). The voucher may also specify whether the recipient computer is permitted during the term of the lending or lease to serve as a sender computer for the specified data item in another usage permission transfer procedure with another recipient computer (e.g., to effectively sub-lend 25 or sub-lease the permission).

In a case of giving or selling, the recipient computer is entitled to retain the secret key indefinitely, and to serve as a sender computer in a subsequent transaction. If at the start of the execution of the usage permission transfer 30 procedure in a giving or selling context the sender computer had permission data to allow only one end-user computer (e.g., itself) to gain access to the data

item, the secret key is erased at the sender computer after the recipient computer is provided with the secret key.

In a case of leasing or selling, the permission may be provided in

5 exchange for funds, the delivery of which may be handled completely independently of the usage permission transfer procedure, or may be handled by another procedure that is tied to the usage permission transfer procedure to help ensure that permission is not provided before the funds are delivered.

10 The sender computer may also create an audit file to permit revenue accounting.

At least because the data item, access to the data item, or both can be transferred from computer to computer (e.g., end-user computer to end-user

15 computer) in accordance with the usage permission transfer procedure, the access or the data item or both are fungible and have a resale value, much as an automobile is fungible and has a resale value. For example, the usage

20 permission transfer procedure makes it possible for an end-user to purchase or lease an instance of access to a book data item from a retailer for five dollars, enjoy the book data item (e.g., by reading the text of the book data item), and then sell the instance of access to another end-user (e.g., for more or less than

25 five dollars, depending on whether the instance has appreciated for a reason such as scarcity or has depreciated for a reason such as a lack of a warranty against corrupted data).

In at least some cases, it is advantageous if at least the audit file, the

30 secret key, the public/private key set, the permission data bank, the group private key, and the de-encryptors at each sender computer and recipient computer are stored and used in a highly secure way, e.g., in a smartcard

computer as described above. If the smartcard computer 46 is used, security is enhanced if the group private key and the smartcard computer's unique private key are never transmitted in any form outside the smartcard computer

5 (i.e., are never presented at the connection circuitry), and if the secret keys are never transmitted in unencrypted form. The encrypted data item may be stored separately from the keys (e.g., in a persistent memory such as a hard disk outside the smartcard computer due to limited data storage space within

10 the smartcard computer). In any case, security is further enhanced if the encrypted data item is de-encrypted in only a piece at a time as necessary (e.g., a page at a time for display purposes).

15 Security may also be enhanced by the use of a secure network connection between the sender computer and the recipient computer. For example, in a specific embodiment, the sender computer includes a Web server computer to which the recipient computer is connected via a network that conforms at least in part to Internet standards such as HTML, HTTP, and

20 TCP/IP (an "Internet network"). See Hyper Text Transfer Protocol – HTTP 1.1. RFC2068. In such a case, security is enhanced if the Internet network connection between the sender computer and the recipient computer operates according to a Secure Sockets Layer ("SSL") standard. See Secure Sockets Layer

25 Specifications 3.0, Netscape, Inc. The Web server may serve as a demand-driven distribution center (e.g., for a publisher, a distributor, or a retailer) from which the recipient computer (e.g., for a distributor, a retailer, or an end-user) can download data items, which may be selectable (e.g., via a Web page on the

30 Web server) at the recipient computer (e.g., running a Web browser). The recipient computer may download software (e.g., display software or software

implementing at least a portion of the usage permission transfer procedure) from the sender computer.

The connection between the sender computer and the recipient computer may be accomplished by one or more wired or wireless data transmission technologies (e.g., modem dialup over telephone lines, cellular telephone, or infrared transmission).

In a specific embodiment, the sender computer or the recipient computer includes a special purpose book viewing computer 110 (Fig. 15) ("book reader") as now described. The book reader is a hand-held, battery-powered device that can be used to display book data (including textual information) clearly, and includes a 32-bit microcomputer (e.g., a Philips Semiconductor PR37100 MIPS processor or an Intel StrongARM 1100 processor, and UCB1200 peripheral control chips) running an operating system such as Microsoft Windows CE 2.1. A portrait-mode liquid crystal display ("LCD") screen 112 with supporting electronics (e.g., a Sharp HR-TFT LQ084V2DS01 8.4-inch VGA (640 x 480) reflective TFT color LCD, driven by an S-MOS Systems SED1355 video controller chip if the PR37100 processor is used) is also included in the book reader, which lacks a keyboard and a mouse. The book reader also has a 4-wire resistive touch screen with anti-glare coating, 16MB DRAM, 8MB Flash ROM for the operating system and built-in software, a compact Flash memory slot with an 8MB flash memory card for book data storage, and an IrDA infrared interface capable of using built-in capabilities of the microcomputer for personal computer connectivity. Further, the book reader has an RJ-11 telephone jack, a DAA and modem interface using built-in capabilities of the microcomputer and Softmodem software for a direct Internet connection, "Next

Page", "Prev Page", "Menu", "Enter", and "Reset" pushbuttons, and a sliding mode switch having "Off", "Read", "Books", "Library", and "Bookstore" positions. Also included in the book reader are four AA batteries (if alkaline, 5 good for more than 40 hours of operation) and an AC-adapter power supply with support for power-conservation modes (e.g., of the microcomputer), a high-quality touch-screen stylus, and a smartcard slot for the smartcard computer.

10 The book reader is packaged to resemble or suggest a leather-bound book, is approximately 8 inches high by 5.25 inches wide, and is as thin and light-weight (e.g., about 1.5 pounds) as is practical in view of the included components. The LCD screen is oriented vertically (i.e., 480 x 640) and an LCD 15 bezel around the LCD screen is as small as practical without unduly degrading durability. The "Next Page" and "Prev Page" pushbuttons are recessed and substantially centered on the right and left sides of the LCD bezel. The "Menu" 20 and related pushbuttons are disposed on the bottom of the LCD bezel. The pushbuttons are comfortable and easy to press, and are nearly completely silent but provide significant tactile feed-back when pressed. The sliding mode switch is recessed and is disposed on the right side of the book reader. The 25 Reset button is deeply recessed so that a ball-point pen or similar device is required to cause activation of the Reset button. An infrared transceiver bezel is disposed on the top edge of the book reader, the RJ-11 and AC power adapter jacks are disposed on the bottom edge of the book reader, and the 30 compact Flash memory slot is disposed on the back of the book reader. The book reader's exterior is made of magnesium, which enhances the aesthetics

and durability of the book reader, and is covered by an attached folding leather cover 114 to protect the book reader and the book reader's LCD screen.

In at least some cases, it is advantageous if the book reader is visually 5 elegant, with fine detailing, includes rich-looking materials (e.g., leather, glass, magnesium) and plastic rubber-like hand grips, and is substantially weather-proof (e.g., has gaskets around the display and the buttons) and highly durable.

10 In other specific embodiments, the sender computer or the recipient computer may include a notebook computer or a desktop computer. In either case, the highly secure mechanism may include highly secure data files or highly secure software or both, or may include a smartcard computer (e.g., 15 attached to a serial, parallel, or USB port, plugged into a PCMCIA smartcard adapter, or integrated in the form of a device embedded on a motherboard).

The technique (i.e., the procedures described above) may be 20 implemented in hardware or software, or a combination of both. In at least some case, it is advantageous if the technique is implemented in computer programs executing on programmable computers (e.g., a personal computer running or able to run Microsoft Windows 95, 98, or NT, or MacIntosh OS) 25 that each include a processor, a storage medium readable by the processor (including volatile and non-volatile memory and/or storage elements), at least one input device such as a keyboard, and at least one output device. Program code is applied to data entered using the input device to perform the method 30 described above and to generate output information. The output information is applied to one or more output devices such as a display screen of the computer.

In at least some cases, it is advantageous if each program is implemented in a high level procedural or object-oriented programming language such as Java or C++ to communicate with a computer system.

5 However, the programs can be implemented in assembly or machine language, if desired. In any case, the language may be a compiled or interpreted language.

In at least some cases, it is advantageous if each such computer program 10 is stored on a storage medium or device (e.g., ROM or magnetic diskette) that is readable by a general or special purpose programmable computer for configuring and operating the computer when the storage medium or device is read by the computer to perform the procedures described in this document.

15 The system may also be considered to be implemented as a computer-readable storage medium, configured with a computer program, where the storage medium so configured causes a computer to operate in a specific and predefined manner.

20 Other embodiments are within the scope of the following claims. For example, the recipient computer may include a desktop or portable computer that includes circuitry (e.g., a dongle that attaches to a port of the computer, or 25 a plug-in or PCMCIA card with memory devices embedded in epoxy) that helps to perform at least some of the functions performed by the smartcard computer as described above. In such a case, the data item may be displayed on the desktop or portable computer's display screen.

30 At least some of the functions performed by the smartcard computer may be performed completely or substantially in software instead, which may not be an arrangement that is as secure as the use of the smartcard computer.

The data item may include any type of data, including the text of a periodical (e.g., a magazine), audio data (e.g., music), or visual data (e.g., still pictures or video).

5 Other techniques may be used to help to prevent unauthorized dissemination of the group private key or the negative consequences of such dissemination. For example, it may be arranged that the group private key is retrievable only by a complex spread-spectrum wireless transfer technique or is 10 otherwise further protected in hardware, or is effective only temporarily.

For a reason such as a reduction in transaction time between the sender computer and the recipient computer, the encrypted data item may be stored in a publicly accessible location (e.g., on the Internet) so that only the 15 permission data need be transferred from the sender computer to the recipient computer. In such a case, the encrypted data item may be freely transferred and copied by anyone, but the permission data is transferred only under the 20 control of the usage permission transfer procedure.

What is claimed is:

1. A method for use in distributing access to a data item,
25 comprising:
allowing multiple transfers between computers of a single instance of
permission to gain access to the data item, the transfers occurring across data
connections and including a first transfer between a first computer and a
30 second computer and a subsequent transfer between the second computer and
a third computer, wherein at any one time only one computer retains the

instance of permission and is able to use the instance of permission to gain access to the data item.

2. The method of claim 1, further comprising:
 - 5 using an encryption key to impede unauthorized access to the data item.
 3. The method of claim 1, wherein at least one of the transfers of permission includes the transfer of a first encryption key.
 4. The method of claim 3, further comprising:
 - 10 using a second encryption key to encrypt the first encryption key prior to transfer.
 5. The method of claim 4, wherein the first encryption key includes a secret key and the second encryption key includes one of the keys in a 15 public/private key set.
 6. The method of claim 1, further comprising:
 - 20 using highly secure circuitry to help ensure that at any one time only one of the computers retains and is able to use the instance.
 7. The method of claim 6, wherein the highly secure circuitry includes a smartcard computer.
 8. The method of claim 6, wherein the highly secure circuitry 25 includes a de-encryptor.
 9. The method of claim 6, further comprising:
 - 20 storing an encryption key in the highly secure circuitry.
 10. The method of claim 9, further comprising:
 - 30 using the encryption key only within the highly secure circuitry.
 11. The method of claim 1, further comprising:

determining whether a computer is authorized to receive the instance of permission to gain access to the data item.

12. The method of claim 1, further comprising:
 - 5 according to an expiration time, rendering at least one of transfers temporary.
 13. The method of claim 12, further comprising:
 - 10 in the temporary transfer, transmitting a copy of an encryption key from a sender computer to a recipient computer, and, at the expiration time, erasing the copy of the encryption key from the recipient computer.
 14. The method of claim 1, further comprising:
 - 15 in one of the transfers, transmitting a copy of an encryption key from a sender computer to a recipient computer, and erasing the copy of the encryption key from the sender computer.
 16. The method of claim 1, further comprising:
 - 20 associating at least one of the transfers with a transfer of funds.
 17. The method of claim 1, further comprising:
 - 25 distinguishing between different instances of permission to gain access to the data item.
 18. The method of claim 1, wherein at least one of the computers includes a Web server computer.
 19. The method of claim 18, wherein the book viewing device includes a viewing screen and data communications circuitry.
 20. A method comprising:

in accordance with access distribution parameters that are specific to a data item and that were established by a first computer, transferring, across a data connection from a second computer to a third computer and

5 independently of the first computer, permission to gain access to the data item.

21. A method comprising:

impeding a change to the number of computers that are allowed to gain access to a data item, independently of data connection transfers between

10 computers of permission to gain access to the data item.

22. A method for use in distributing access to a data item, comprising:

providing a first computer with permission to gain access to the data

15 item;

providing the permission by data connection to a second computer substantially simultaneously with removing the permission from the first

20 computer; and

providing the permission by data connection to a third computer substantially simultaneously with removing the permission from the second computer.

25 23. A method comprising:

rendering accountably fungible an instance of permission data that allows a computer to gain access to book data.

24. A method for use in distributing access to a book data item,

30 comprising:

associating highly secure circuitry with a device that is able to send and receive access data that is necessary to gain access to the book data item, the

highly secure circuitry including a computer processor and a program memory and being able to substantially prevent an unauthorized transfer of the access data from the device.

5 25. A method for use in distributing access to a book data item, comprising:

 at a publisher computer, storing publisher permission data that allows a number A of end-user computers to gain access to the book data item;

10 based on the publisher permission data, providing a distributor computer with distributor permission data that allows a number B of end-user computers to gain access to the book data item;

 changing the publisher permission data so that the publisher permission data allows only a number A-B of end-user computers to gain access to the book data item;

15 based on the distributor permission data, providing a retailer computer with retailer permission data that allows a number C of end-user computers to gain access to the book data item;

 changing the distribution permission data so that the distributor permission data allows only a number B-C of end-user computers to gain access to the book data item;

20 based on the retailer permission data, providing an end-user computer with end-user permission data that allows 1 end-user computer to gain access to the book data item; and

25 changing the retailer permission data so that the retailer permission data allows only a number C-1 of end-user computers to gain access to the book data item.

26. A system for use in distributing access to a data item, comprising:
data processing apparatus for allowing multiple transfers between
computers of a single instance of permission to gain access to the data item,
5 the transfers occurring across data connections and including a first transfer
between a first computer and a second computer and a subsequent transfer
between the second computer and a third computer, wherein at any one time
only one computer retains the instance of permission and is able to use the
10 instance of permission to gain access to the data item.

27. A system comprising:
a transferor, in accordance with access distribution parameters that are
specific to a data item and that were established by a first computer,
15 transferring, across a data connection from a second computer to a third
computer and independently of the first computer, permission to gain access to
the data item.

28. A system comprising:
an impedor impeding a change to the number of computers that are
allowed to gain access to a data item, independently of data connection
transfers between computers of permission to gain access to the data item.

29. A system for use in distributing access to a data item, comprising:
a first permission provider providing a first computer with permission
to gain access to the data item;
a second permission provider providing the permission by data
30 connection to a second computer substantially simultaneously with removing
the permission from the first computer; and

a third permission provider providing the permission by data connection to a third computer substantially simultaneously with removing the permission from the second computer.

5 30. A system comprising:

a renderor rendering accountably fungible an instance of permission data that allows a computer to gain access to book data.

10 31. A system for use in distributing access to a book data item, comprising:

a device including highly secure circuitry, the device being able to send and receive access data that is necessary to gain access to the book data item, the highly secure circuitry including a computer processor and a program 15 memory and being able to substantially prevent an unauthorized transfer of the access data from the device.

20 32. A system for use in distributing access to a book data item, comprising:

at a publisher computer, a storer for storing publisher permission data that allows a number A of end-user computers to gain access to the book data item;

25 a first permission provider for, based on the publisher permission data, providing a distributor computer with distributor permission data that allows a number B of end-user computers to gain access to the book data item;

30 a first permission changer for changing the publisher permission data so that the publisher permission data allows only a number A-B of end-user computers to gain access to the book data item;

a second permission provider for, based on the distributor permission data, providing a retailer computer with retailer permission data that allows a number C of end-user computers to gain access to the book data item;

5 a second changer for changing the distribution permission data so that the distributor permission data allows only a number B-C of end-user computers to gain access to the book data item;

10 a third permission provider for, based on the retailer permission data, providing an end-user computer with end-user permission data that allows 1 end-user computer to gain access to the book data item; and

15 a third changer for changing the retailer permission data so that the retailer permission data allows only a number C-1 of end-user computers to gain access to the book data item.

33. Computer software, residing on a computer-readable medium, comprising instructions for use in distributing access to a data item, the 20 instructions causing a computer to:

allow multiple transfers between computers of a single instance of permission to gain access to the data item, the transfers occurring across data connections and including a first transfer between a first computer and a second computer and a subsequent transfer between the second computer and a third computer, wherein at any one time only one computer retains the instance of permission and is able to use the instance of permission to gain access to the data item.

34. Computer software, residing on a computer-readable medium, comprising instructions for causing a computer to:

in accordance with access distribution parameters that are specific to a data item and that were established by a first computer, transfer, across a data connection from a second computer to a third computer and independently of 5 the first computer, permission to gain access to the data item.

35. Computer software, residing on a computer-readable medium, comprising instructions for causing a computer to: 10
impede a change to the number of computers that are allowed to gain access to a data item, independently of data connection transfers between 15 computers of permission to gain access to the data item.

36. Computer software, residing on a computer-readable medium, comprising instructions for use in distributing access to a data item, the 15 instructions causing a computer to:
provide a first computer with permission to gain access to the data item; 20
provide the permission by data connection to a second computer substantially simultaneously with removing the permission from the first computer;

25 provide the permission by data connection to a third computer substantially simultaneously with removing the permission from the second computer.

37. Computer software, residing on a computer-readable medium, comprising instructions for causing a computer to: 30
render accountably fungible an instance of permission data that allows a computer to gain access to book data.

38. Computer software, residing on a computer-readable medium, comprising instructions for use in distributing access to a book data item, the instructions causing a computer to:

5 associate highly secure circuitry with a device that is able to send and receive access data that is necessary to gain access to the book data item, the highly secure circuitry including a computer processor and a program memory and being able to substantially prevent an unauthorized transfer of the access
10 data from the device.

39. Computer software, residing on a computer-readable medium, comprising instructions for use in distributing access to a book data item, the instructions causing a computer to:

15 at a publisher computer, store publisher permission data that allows a number A of end-user computers to gain access to the book data item; based on the publisher permission data, provide a distributor computer
20 with distributor permission data that allows a number B of end-user computers to gain access to the book data item;

change the publisher permission data so that the publisher permission data allows only a number A-B of end-user computers to gain access to the
25 book data item;

based on the distributor permission data, provide a retailer computer with retailer permission data that allows a number C of end-user computers to gain access to the book data item;

30 change the distribution permission data so that the distributor permission data allows only a number B-C of end-user computers to gain access to the book data item;

based on the retailer permission data, provide an end-user computer with end-user permission data that allows 1 end-user computer to gain access to the book data item; and

5 change the retailer permission data so that the retailer permission data allows only a number C-1 of end-user computers to gain access to the book data item.

10

15

20

25

30

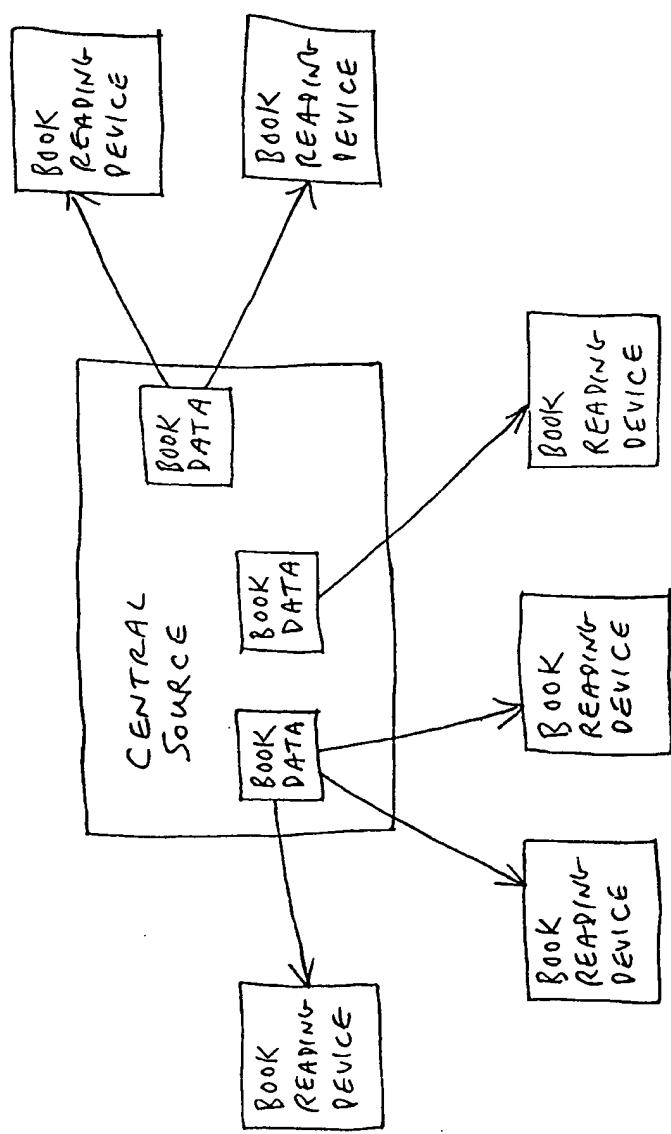


FIG. 1 (PRIOR ART)

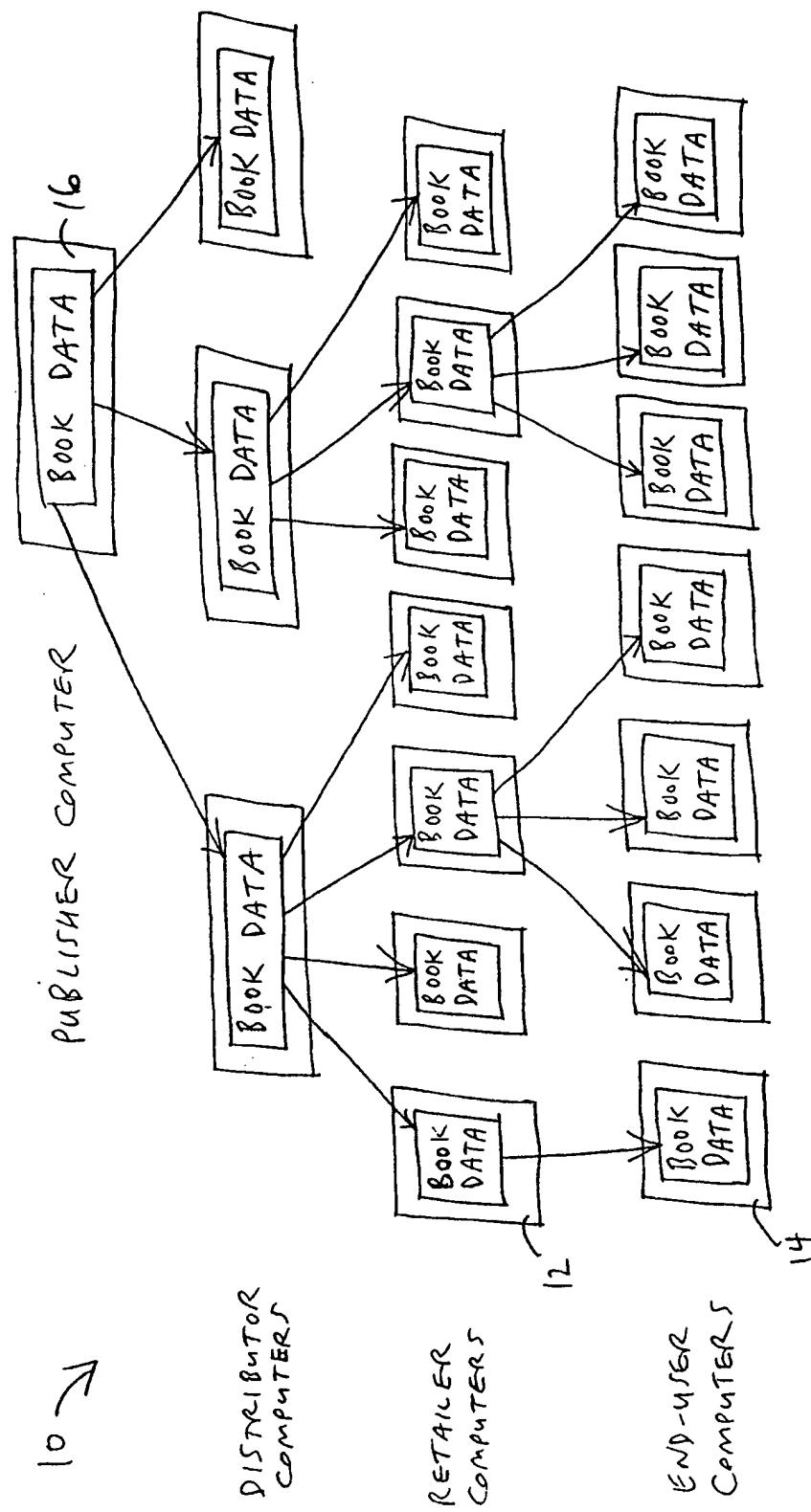


FIG. 2

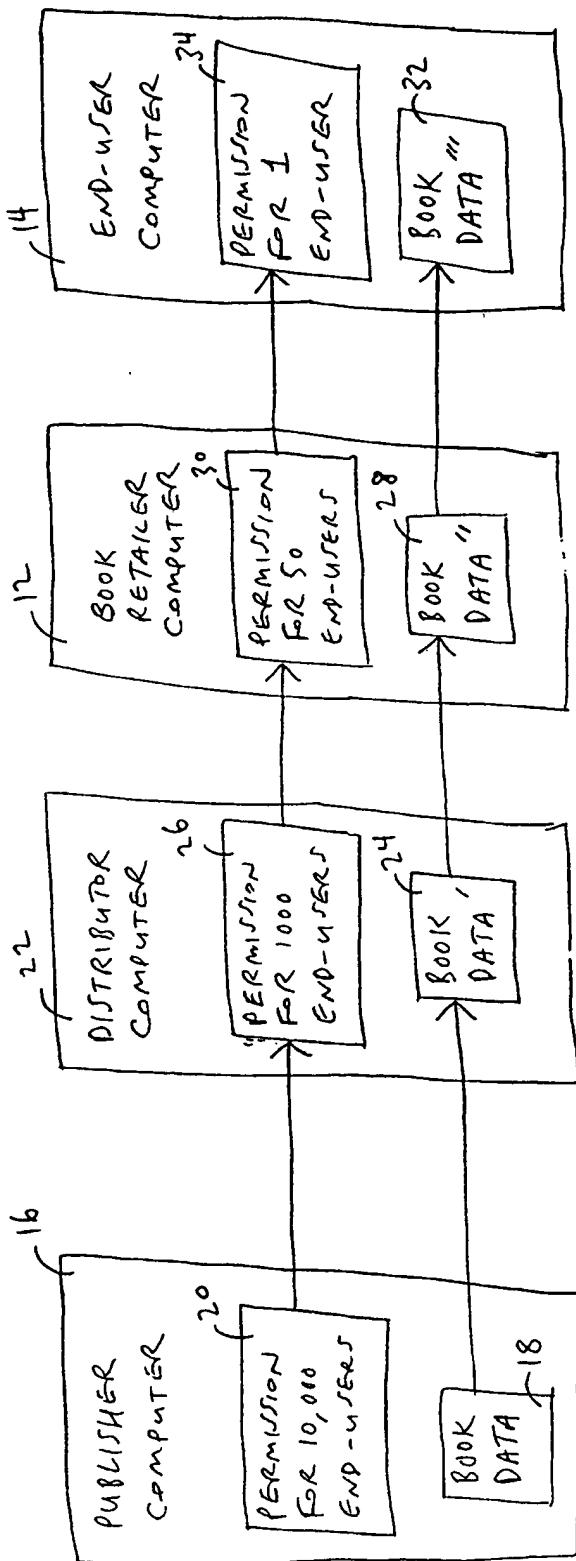


FIG. 3

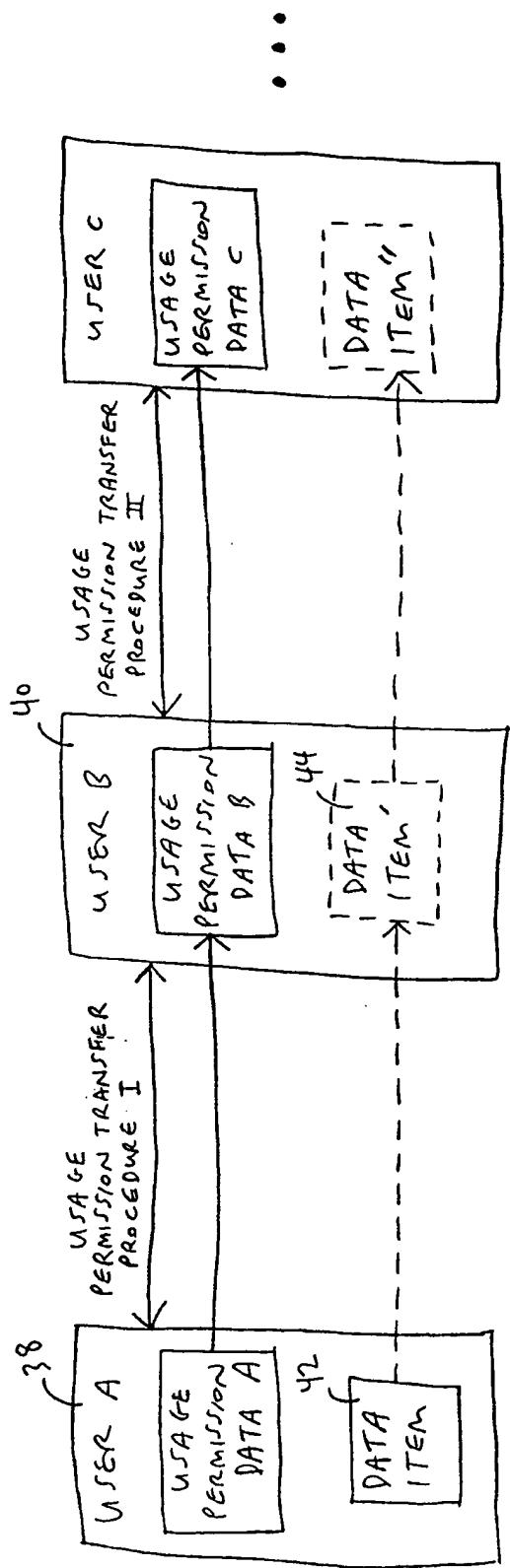


FIG. 4

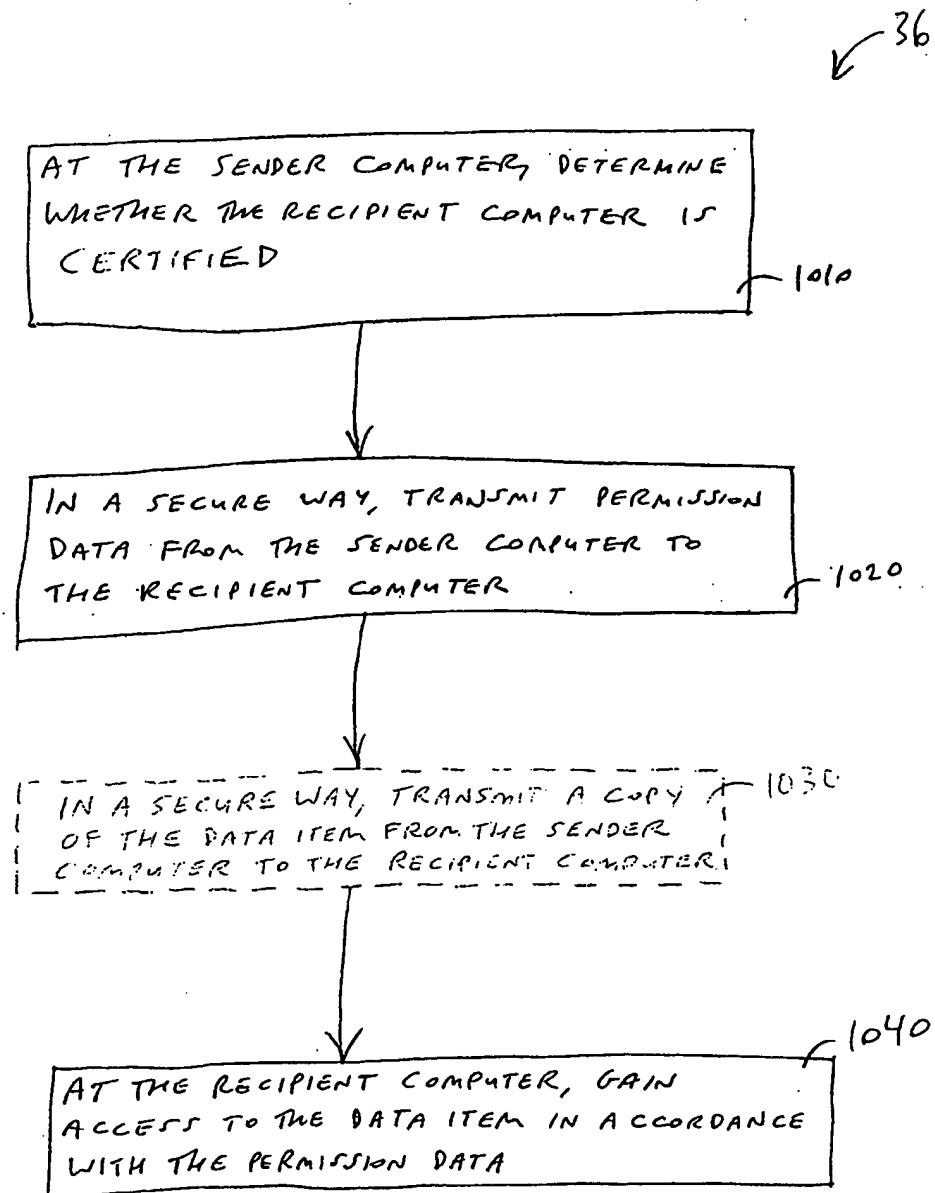


FIG. 5

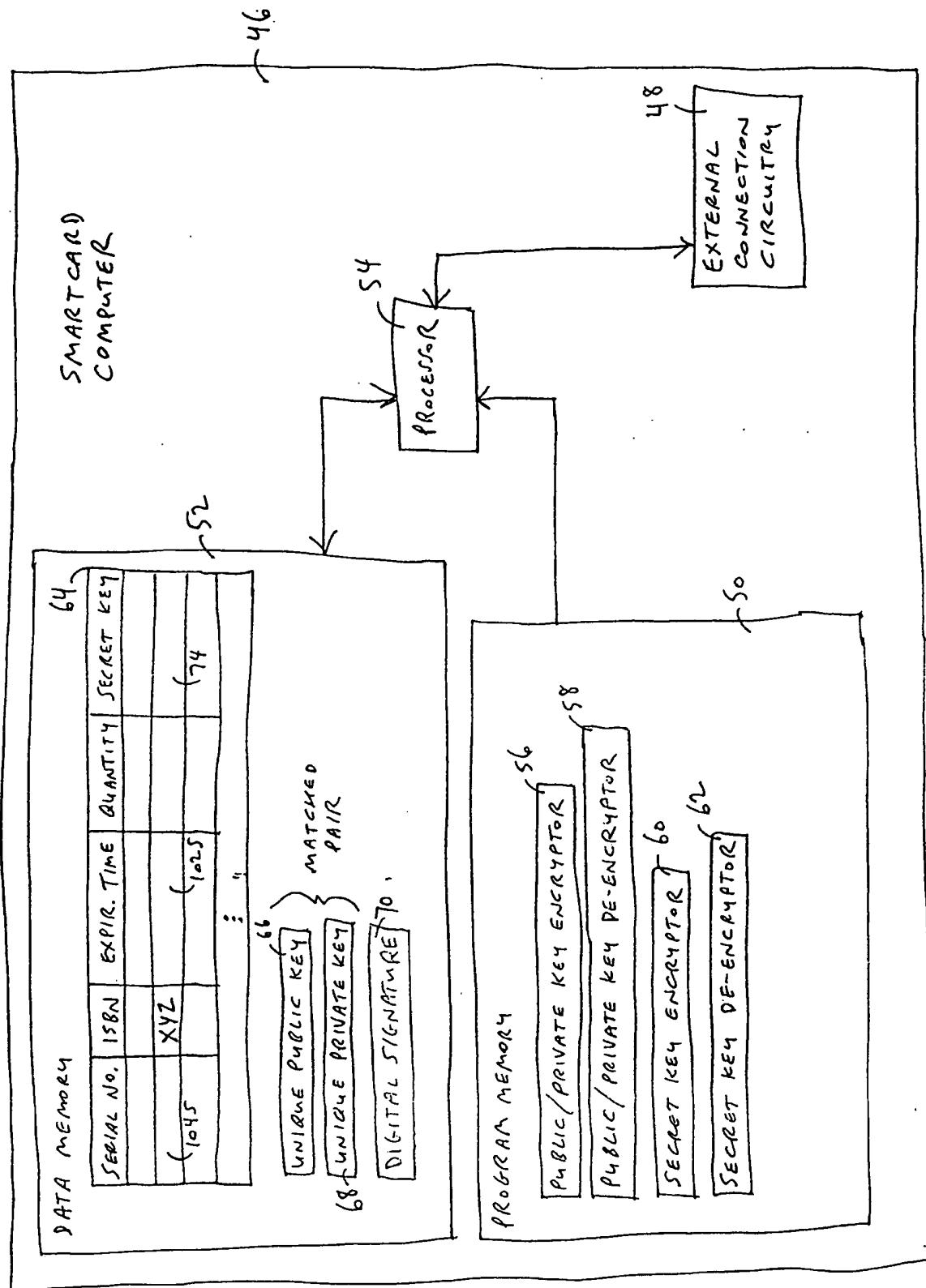


FIG. 6

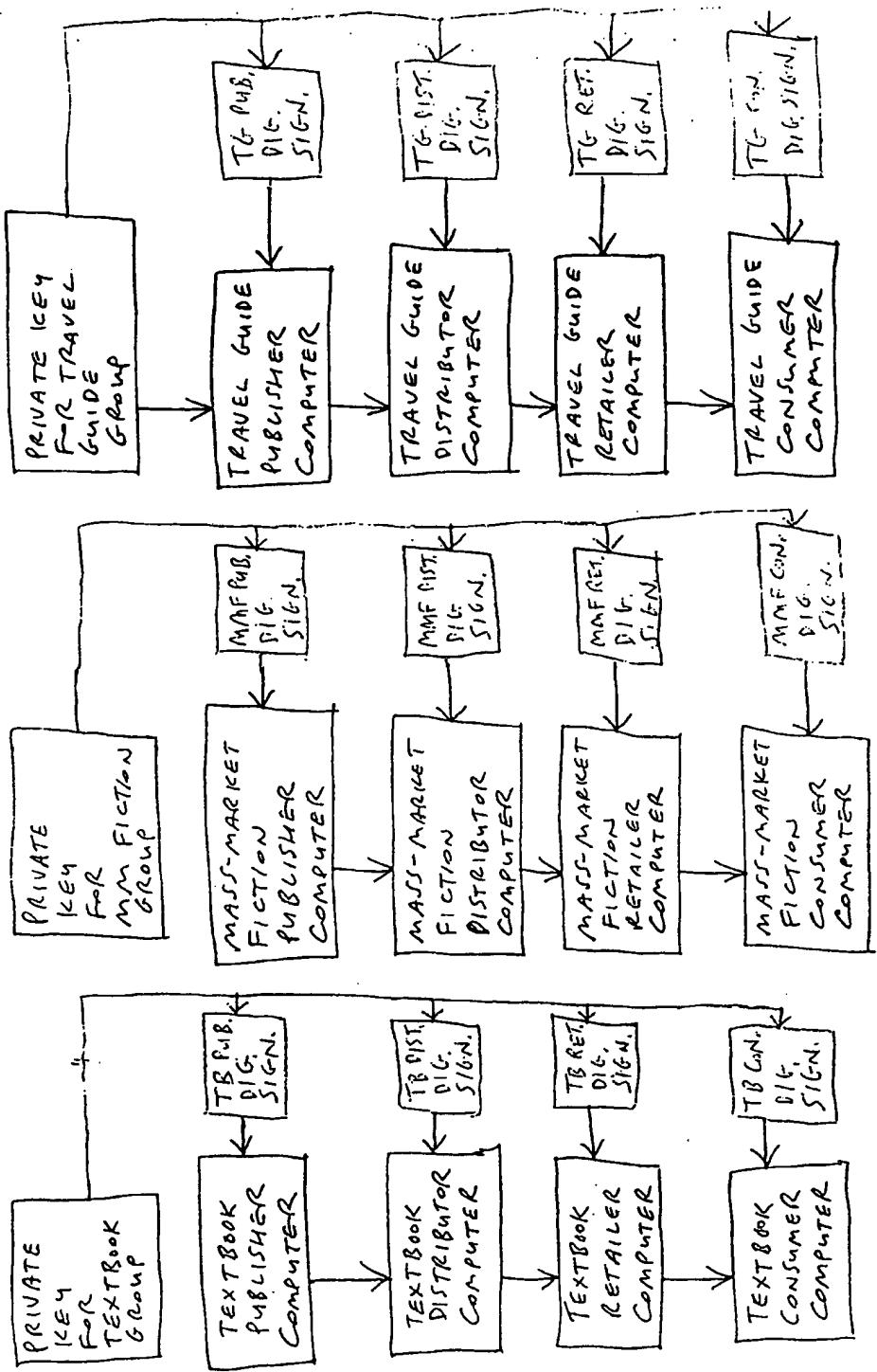


FIG. 7

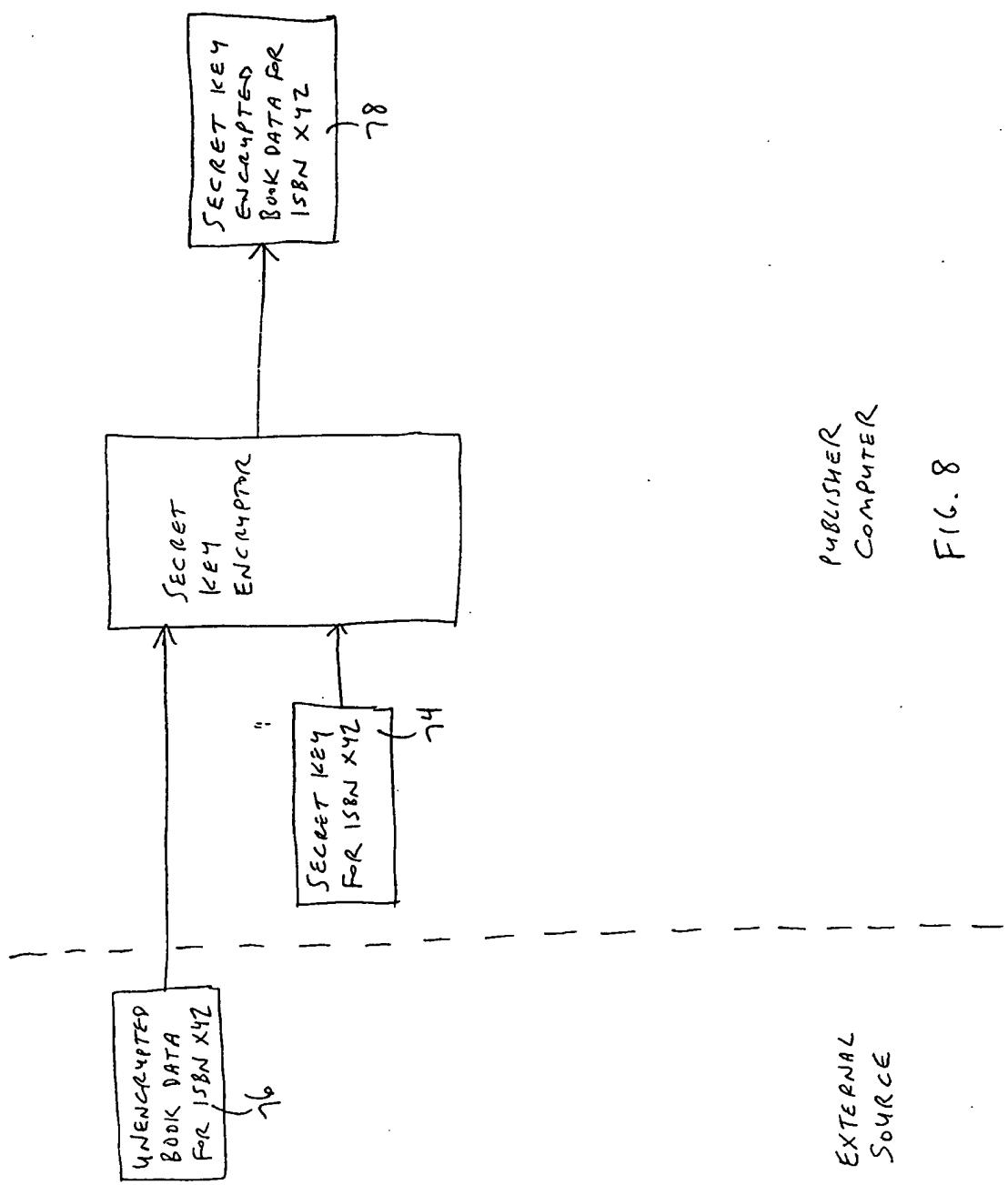
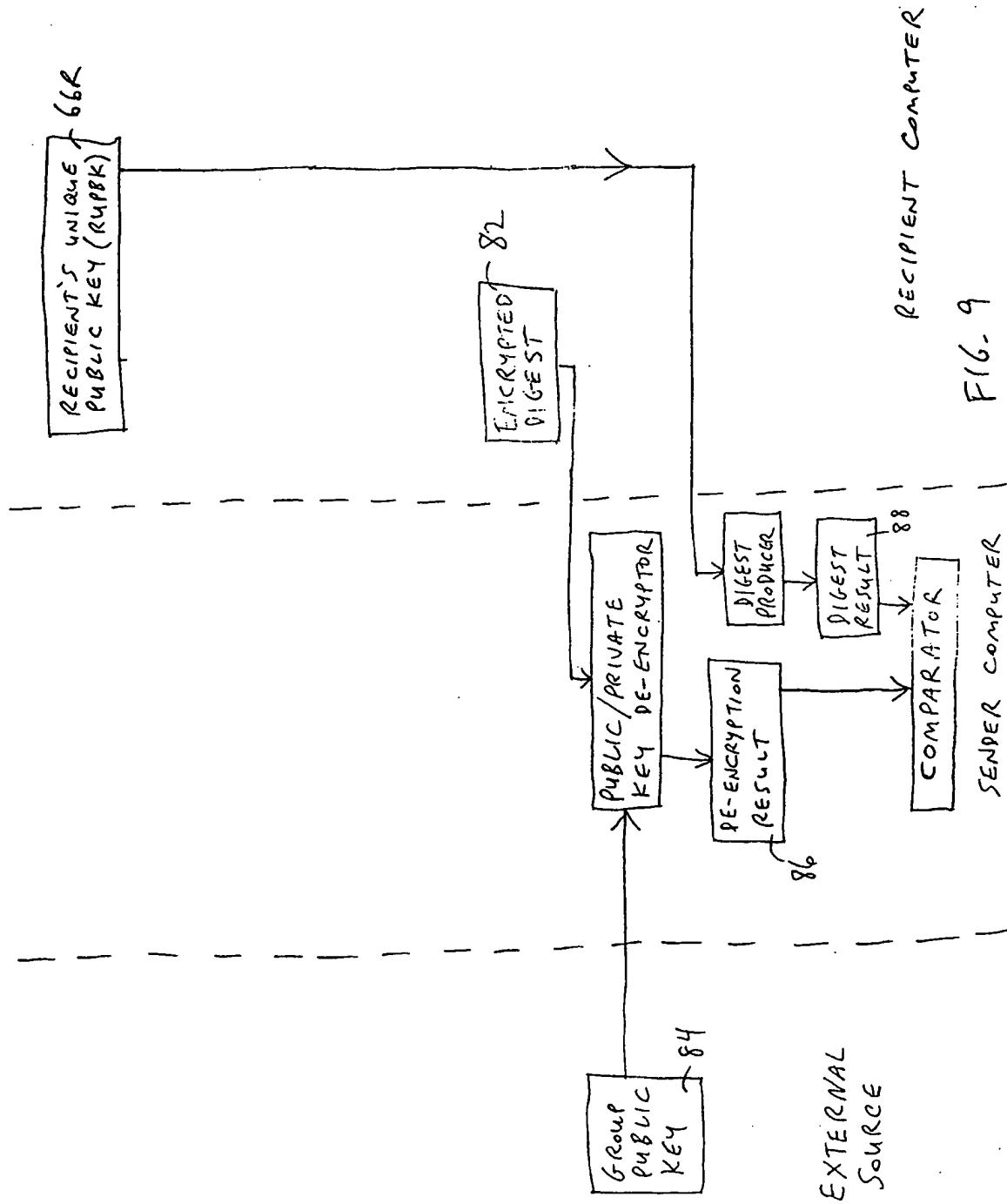
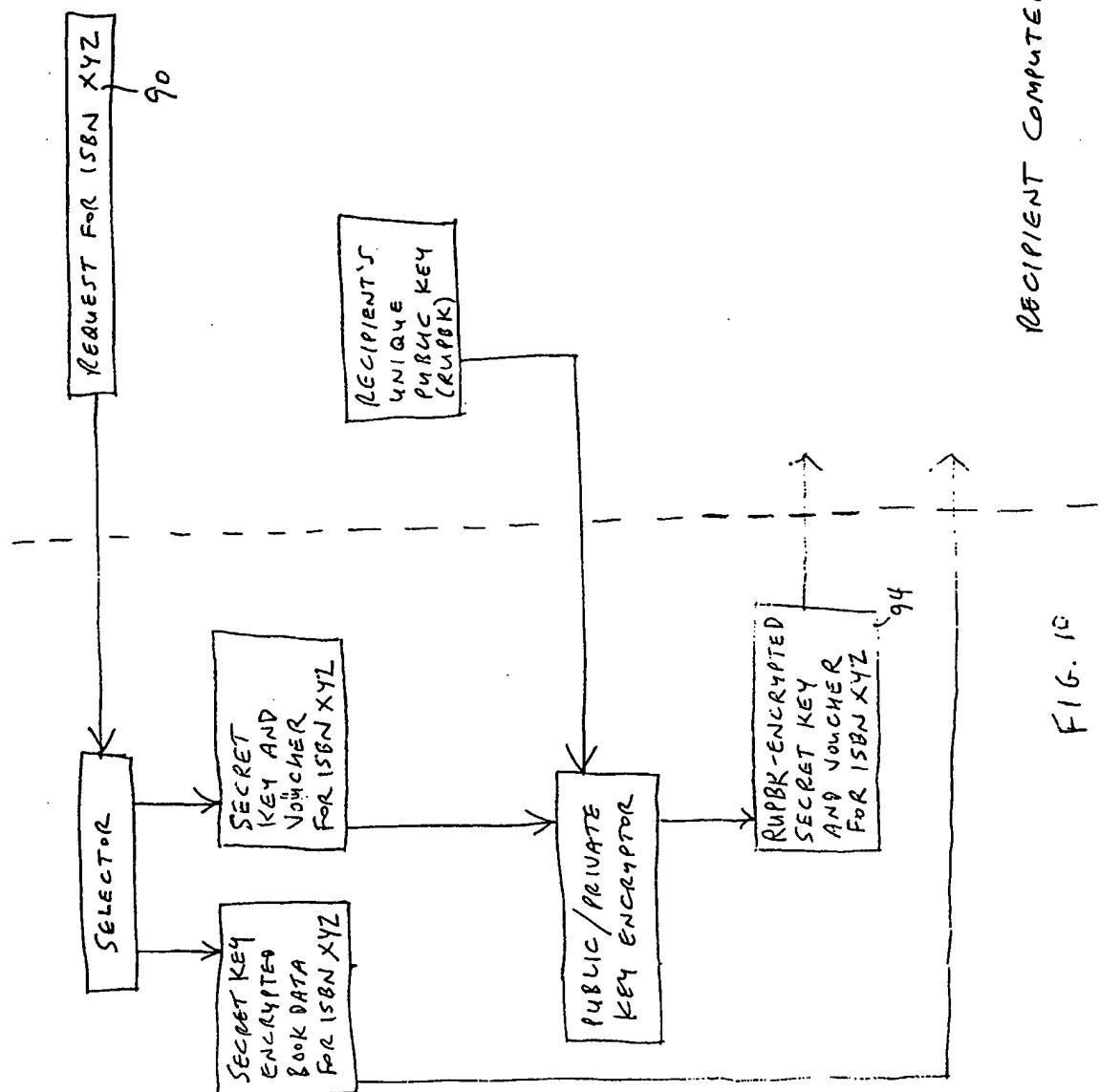


FIG. 8





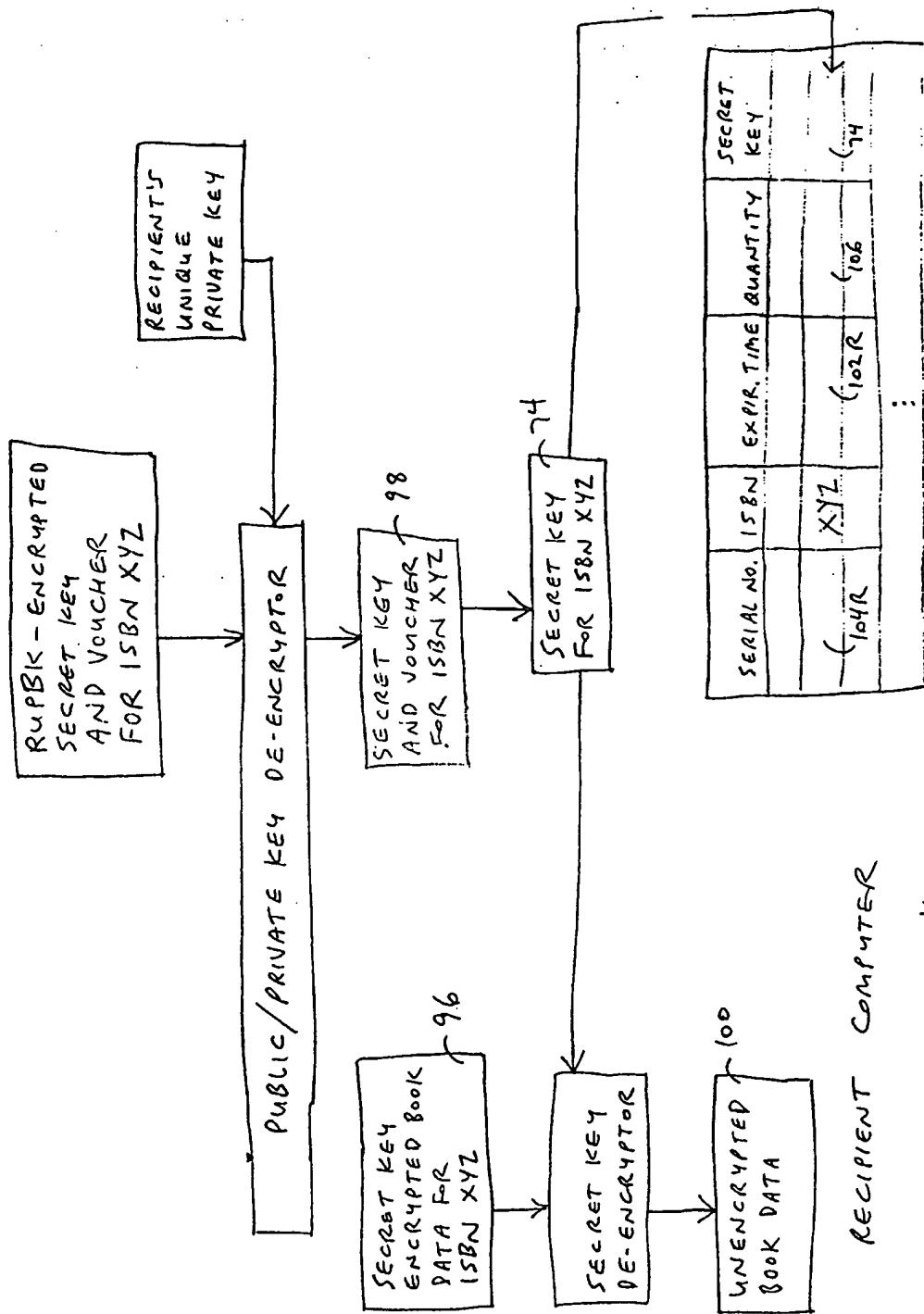


FIG. 11

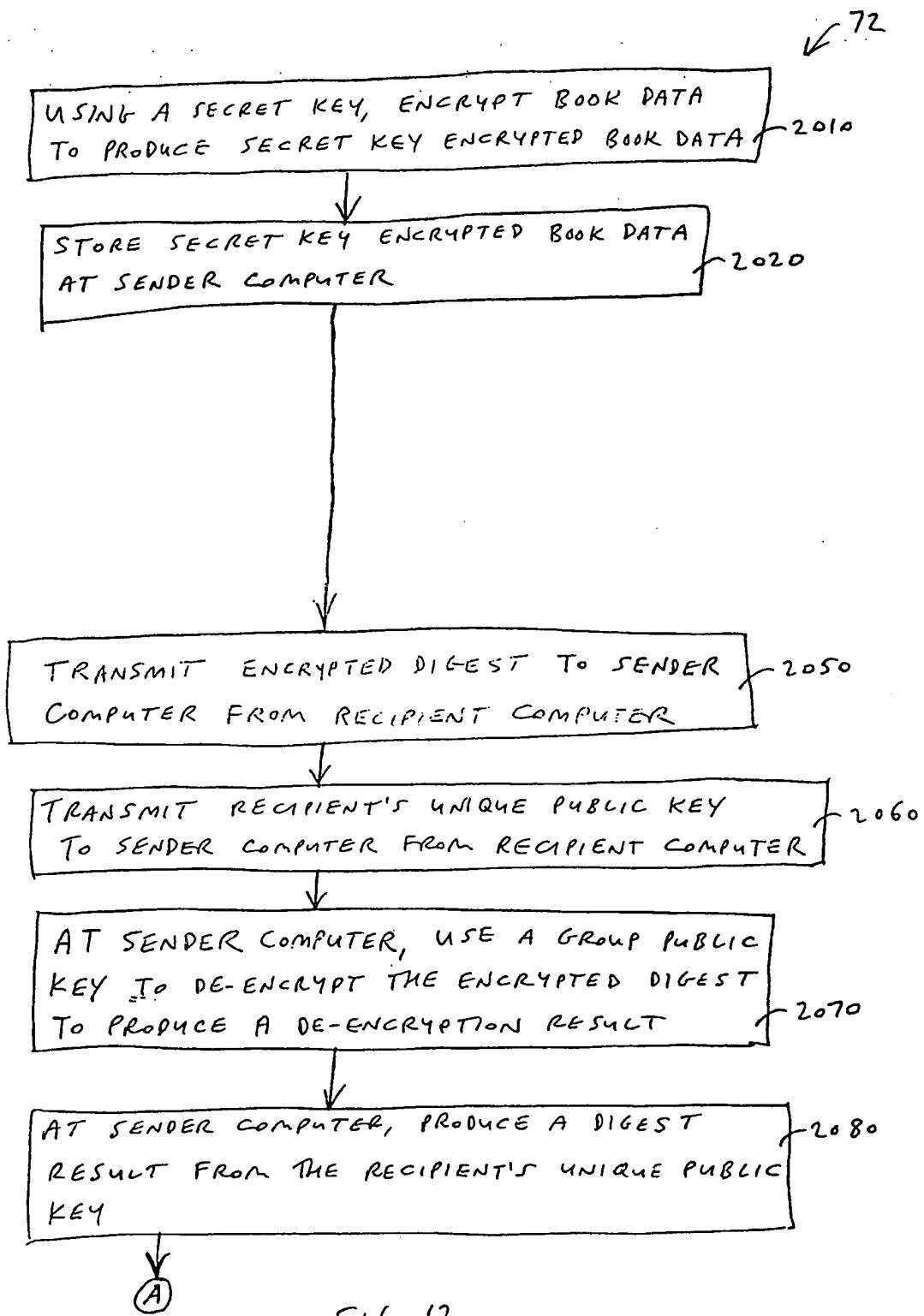
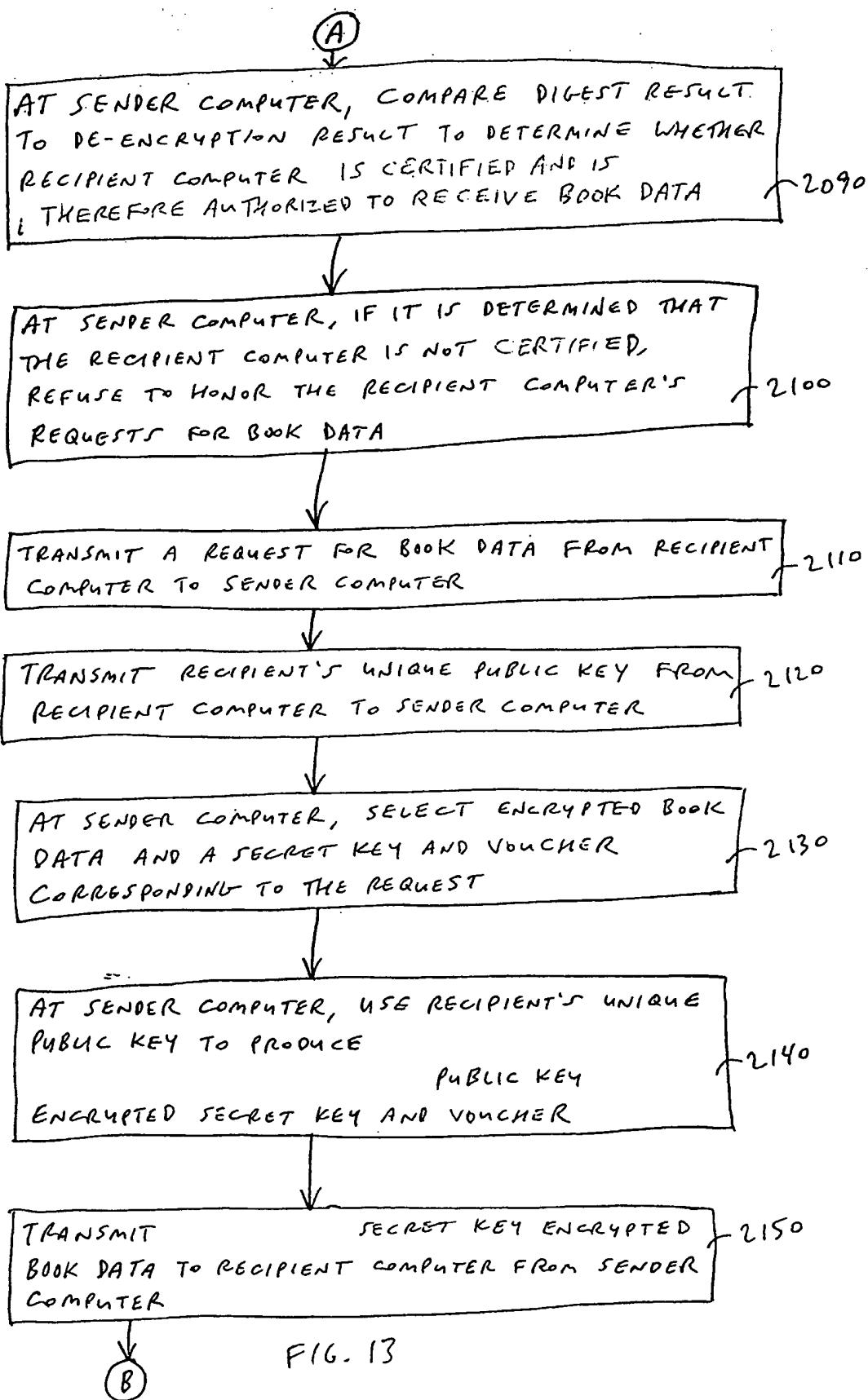


FIG. 12



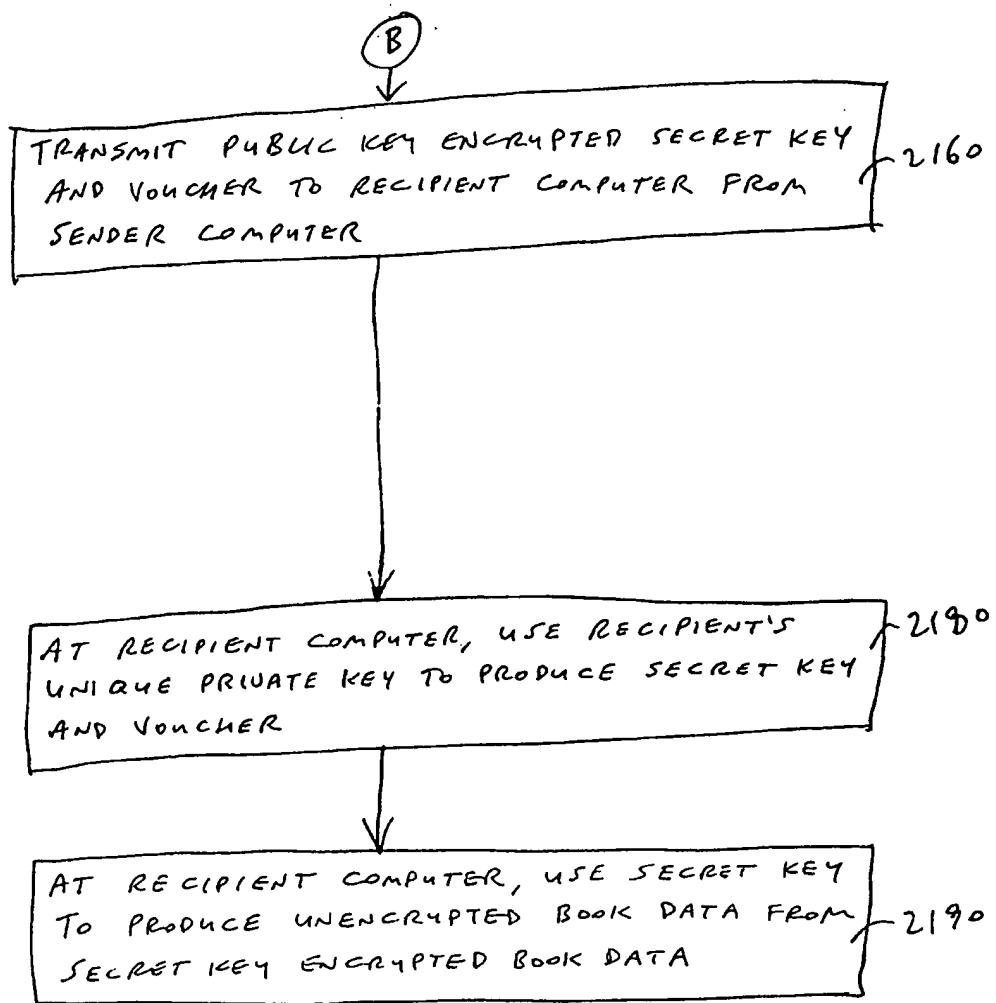


FIG. 14

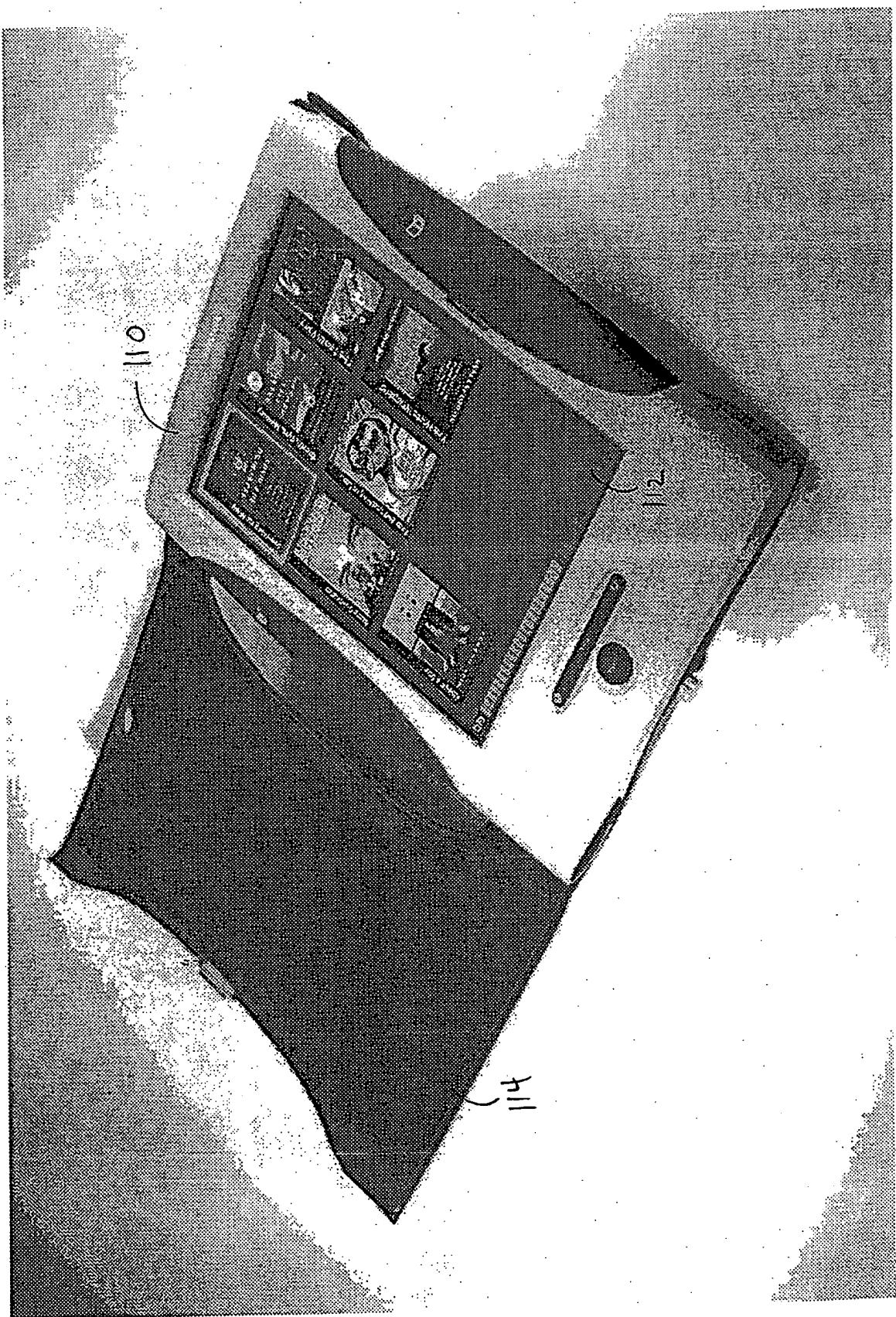


FIG. 15

INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 99/23474

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 08344 A (THE VIRTUAL PRESS) 26 February 1998 (1998-02-26) page 5, line 1 -page 7, line 27 page 9, line 18 - line 21; figures 1,2A,2B	23,30
A	---	1-3,11, 15-19,24
X	EP 0 695 997 A (AT&T CORP.) 7 February 1996 (1996-02-07) page 3, line 25 -page 4, line 44; figures 1,2	23,30
A	---	1-5,11, 15,31
X	EP 0 715 245 A (XEROX CORP.) 5 June 1996 (1996-06-05) page 6, line 45 - line 57	23,30
A	abstract; figures 1,2,4B,14,16 ---	1,2,11, 15,16, 20,24,27
		-/-

 Further documents are listed in the continuation of box C. Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

& document member of the same patent family

Date of the actual completion of the international search

7 February 2000

Date of mailing of the international search report

10.02.00

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl
Fax: (+31-70) 340-3016

Authorized officer

Taylor, P

INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 99/23474

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 734 823 A (SAIGH ET AL.) 31 March 1998 (1998-03-31)	23,30
A	column 1, line 53 -column 2, line 55; figures 3,4,9,12	1,15-17, 20,24, 25,31,32
A	---	
	WO 96 27155 A (ELECTRONIC PUBLISHING RESOURCES LTD.) 6 September 1996 (1996-09-06)	1-5,11, 12, 15-17, 20,24, 27,31
	page 156, line 10 -page 157, line 14 page 189, line 14 -page 191, line 9; figures 1,6,9,62-64,78-80,86,86A	-----

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 99/23474

Patent document cited in search report	Publication date	Patent family member(s)			Publication date
WO 9808344	A 26-02-1998	US 5956034 A			21-09-1999
		AU 4148197 A			06-03-1998
EP 695997	A 07-02-1996	US 5719938 A			17-02-1998
		CA 2151851 A			02-02-1996
		JP 8063436 A			08-03-1996
EP 715245	A 05-06-1996	US 5629980 A			13-05-1997
		JP 8263441 A			11-10-1996
US 5734823	A 31-03-1998	US 5734891 A			31-03-1998
		WO 9309490 A			13-05-1993
WO 9627155	A 06-09-1996	AU 711733 B			21-10-1999
		AU 6326696 A			18-09-1996
		CA 2212574 A			06-09-1996
		CN 1183841 A			03-06-1998
		EP 0861461 A			02-09-1998
		JP 10512074 T			17-11-1998
		US 5910987 A			08-06-1999
		US 5949876 A			07-09-1999
		US 5915019 A			22-06-1999
		US 5917912 A			29-06-1999
		US 5982891 A			09-11-1999

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.